

CLAIMS

1 1. A method of connecting a mobile host to a remote network through
2 an access network with a single user password, where the access network may be
3 independent of the remote network in terms of no protocol conversation between
4 authentication servers in the access network and the remote network, respectively,
5 and a virtual single account (VSA) has been set up for a user to connect to the
6 access network and then to the remote network, comprising the steps of:

7 generating a VSA password and decryption key from the single
8 password received from the user;

9 decrypting at least one of a local access network authentication
10 credential and a remote access authentication credential;

11 initiating a local access network connection; and

12 initiating a remote network access connection.

1 2. The method recited in Claim 1, further comprising the step of
2 initiating a VSA configuration update process with a VSA server.

1 3. The method recited in Claim 2, wherein the VSA configuration
2 update process comprises the steps of:

3 constructing a VSA information update request message;

4 sending the VSA information update request message to the VSA
5 server; and

6 receiving a VSA information update response message from the
7 VSA server.

1 4. The method recited in Claim 3, wherein the VSA information
2 update request message contains an instruction authorizing the step of decrypting
3 the remote network authentication credential prior to initiating the remote network
4 access connection.

1 5. The method recited in Claim 1, further comprising the step of
2 selecting a local access network from a current VSA access record.

1 6. The method recited in Claim 1, further comprising the step of
2 generating the decryption key in response to a random sequence received from the
3 user.

1 7. The method recited in Claim 1, wherein the VSA password is
2 generated using the expression: VSA password = hash(VSA username || common
3 password || VSA server || remote network ID), wherein the VSA username
4 identifies the user to a VSA server, the common password is the single password
5 from the user, and the remote network ID identifies the remote network serving as
6 a home network for the mobile host.

1 8. The method recited in Claim 3, wherein the VSA update request
2 message "Q" is derived from the expression: $Q = \text{VSA username} \parallel X \parallel E_{K1}$
3 (Synchronization time || Request content), where X is a random sequence; and K1
4 is an encryption key calculated from hash (hash (VSA password) || X).

1 9. The method recited in Claim 8, wherein the VSA information
2 update response message "A" is derived from the expression: $A = \text{Response Code}$
3 || Y || E_{K2} (Synchronization time || Response content), wherein Y is a random

4 sequence, and K2 is an encryption key calculated from hash (hash (VSA
5 password) || Y).

1 10. The method recited in Claim 1, further comprising the steps of
2 selecting local access parameters and remote access parameters from a VSA
3 access record.

1 11. A method of connecting a mobile host to a remote network through
2 an access network with a single password, where the access network may be
3 independent of the remote network in terms of no protocol conversation between
4 authentication servers in the access network and the remote network, respectively,
5 and a virtual single account (VSA) has been set up for a user to connect to the
6 access network and then to the remote network, and a VSA server is deployed in
7 the remote network, comprising the steps of:

8 receiving a VSA information update request message from the mobile
9 host;

10 sending a VSA information update response message to the mobile host;

11 receiving an authentication credential for the remote network;

12 verifying the authentication credential; and

13 granting remote network access to the mobile host.

1 12. The method recited in Claim 11, wherein the VSA information
2 update request message "Q" is derived from the expression: $Q = \text{VSA username}$
3 $\parallel X \parallel E_{K1}(\text{Synchronization time} \parallel \text{Request content})$, where X is a random
4 sequence; and K1 is an encryption key calculated from hash (hash (VSA
5 password) || X); and the VSA information update response message "A" is

6 derived from the expression: $A = \text{Response Code} \parallel Y \parallel E_{K2}(\text{Synchronization time}$
7 $\parallel \text{Response content})$, wherein Y is a random sequence, and $K2$ is an encryption
8 key calculated from hash (hash (VSA password) $\parallel Y$).

1 13. The method recited in Claim 11, wherein the VSA server contains
2 a plurality of VSA management records, each management record including a
3 user's VSA authentication credential.

1 14. The method recited in Claim 11, wherein the user's VSA
2 authentication credential includes a VSA password generated from the single user
3 password.

1 15. The method recited in Claim 14, wherein the VSA password is
2 generated using the expression: $\text{VSA password} = \text{hash}(\text{VSA username} \parallel \text{common}$
3 $\text{password} \parallel \text{VSA server} \parallel \text{remote network ID})$, wherein the VSA username
4 identifies a user to a VSA server, the common password is the single password
5 from the user, and the remote network ID identifies the remote network serving as
6 a home network for the mobile host.

1 16. The method recited in Claim 11, wherein the VSA server maintains
2 access information for at least one local access network and at least one remote
3 network.

1 17. The method recited in Claim 14, wherein the access information
2 includes client information for mobile hosts, and management information for at
3 least one additional VSA server.

- 1 18. The method recited in Claim 11, further comprising the step of a
- 2 VSA server signaling a remote access gateway to verify the remote authentication
- 3 credential.